UNITED STATES DISTRICT COURT FOR THE
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	
v.	CASE NO. 04CR10217GAO
DARREN F. WILDER	

AFFIDAVIT OF PETER CHARLES HORSTMANN, ESQUIRE

I, Peter Charles Horstmann, depose and state the following:

1. I am the attorney of record for the Defendant in the instant matter.

2. I submit this Affidavit in support of the Defendant's Motion in Limine to Preclude Evidence and Testimony Regarding EnCase Forensic Software.

3. Both the Government and the Defendant have cited to a 2003 Department of Justice "DOJ" Report concerning DOJ testing performed on EnCase forensic software.

4. I have reviewed the 2003 DOJ Report and believe that is raises more questions than it answers and does not address the recovery of deleted files, which is the primary reason why it was cited in the Defendant's Motion in Limine.

5. Moreover, at a hearing pursuant to Daubert v.Merrell Dow Pharmecuticals, Inc., 509 U.S. 579 (1993), I would ask the following questions of Government experts regarding the DOJ Report and EnCase forensic software.

   a. In addition to allegedly recovering image files from a computer hard drive, how does the software recover and attach the name of a file, the date the

file was created, any dates the file was accessed and the date a file was deleted?

b. Is this information stored separately from the image on a computer hard drive?

c. Are there any studies regarding the accuracy of the recovery of image files, image file names and dates of creation, access and/or deletion?

d. How does EnCase distinguish between files which have been deleted and overwritten on several occasions and correctly apply dates to those files?

e. How does EnCase distinguish between different files which were give the same file name at different times and deleted at different times.

f. How does EnCase distinguish between file names and dates of files which have been overwritten in the same memory space on the hard drive?

g. It appears that the Defendant's hard drive, a Vectra hard drive, is not on the list of hard drives which were tested by the DOJ. Table 5-3, on page 26. Why not?

h. What impact could this have on the reliability of any analysis conducted on a Vectra hard drive and does the DOJ's failure to include Vectra hard drives in the study invalidate any of its findings?

i. On page 11 of the DOJ Report it is noted and is it true that deleted file recovery tools were not part of the DOJ test and "will be tested separately".

j. Considering the fact that the instant case concerns predominantly deleted

files, has the EnCase software been tested separately as suggested by the DOJ Report and what impact the lack of any testing has on the methodology and reliability of the results obtained in the instant case?

k. On page 28 of the 2003 DOJ Report, it is noted that EnCase was run using additional software called SF-TST Release 1.0. Why?

l. Has SF-TST Release 1.0 been separately tested by the DOJ and if so, what are the results?

m. Additionally, the 2003 DOJ Report suggests that 164 tests were run according to the numbering system DI 001-164. See page 11. Is this true?

n. If so, why does the report only contains the results of 51 of the 164 tests?

o. What were the results of these tests and what is the significance of the omission of the 113 other test results from the final DOJ report?

p. What is the reason DI-154 was omitted from the page 92 list of test cases showing “image verification errors”?

q. The 2003 DOJ Report lists 12 errors in the 51 tests reported and what exactly were the errors?

r. What is the significance of this error ratio and were errors found in the other 113 tests which were omitted from the report?

s. What does it mean on page 25 of the DOJ Report that in 25 of the 51 tests reported “expected results not achieved”?

t. What affect does this result have on the overall reliability of EnCase and what were the results of the other 113 tests which were omitted from the

report with respect to results not achieved?

u. Many of the "date of test" and "computer system" clock dates do not match.

v. What affect does this inconsistency have on the overall reliability of the EnCase computer software and, in particular, what impact does it have on the dates reported in the instant case that deleted files were allegedly crated, accessed and deleted.

5. Given these lurking questions about the reliability of the EnCase computer forensic software, an evidentiary hearing pursuant to Daubert is required.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 8TH DAY OF MARCH, 2006.

Peter Charles Horstmann, Esquire